Part 1. Software Security

Tia C

1. Abstract

ScottishGlen asked the author to identify potential vulnerabilities that the hacktivists may be able to exploit. There are several systems that they may attempt to exploit, however the Kerberos network authentication systems is likely to pose the greatest risk to the company. This is due to the fact that if the hackers gain access the network, they can access sensitive information from across the company's network as well as potentially cause damage to systems and data.

The investigator looked into three CVE's that have a high severity base score as well as attack techniques regularly used by attackers. Once the vulnerabilities and potential attack techniques had been covered, mitigations that should be employed within the system were discussed.

2. Introduction

This investigation aims to identify potential vulnerabilities within the Kerberos network authentication system in use at the company's business. The Kerberos network authentication system is an authentication protocol for networks and makes use of three secret keys to authenticate. Kerberos is a stronger authentication protocol than SSH and NTLM due to the stronger encryption that is employed and uses third-party authentication.

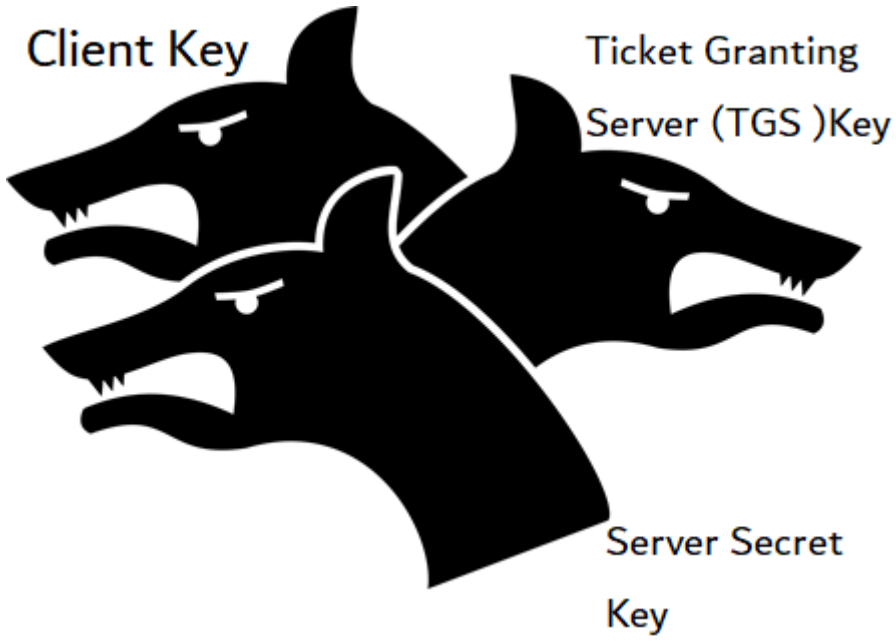

Figure 1 - Kerberos and the three keys it represents

Despite being one of the most secure authentication protocols available, it is still vulnerable to malware and vulnerabilities. If the attackers were able to gain access to the network, they may be able to escalate their privileges within the network to an admin or super user. They can also access sensitive information from across the network as well as potentially causing damage to systems and data.

3. CVEs for Kerberos

CVE is an abbreviation for Common Vulnerabilities and Exposures. The CVE program is run by the MITRE corporation and is used to "identify, define and catalogue publicly disclosed cybersecurity vulnerabilities." (MITRE, 2022). It allows for better vulnerability identification due to the use of CVE ID's which can be used by organisation's security team when doing vulnerability scans. The CVE IDs

are also used when vendors apply security patches and advisories, so security teams can implement mitigations for these vulnerabilities.

3.1 CVE-2020-25719

This vulnerability affects Samba being used in the Active Directory in Red Hat, which is likely employed within the network, it has a **high** severity score of 7.2. The weakness enumeration of the vulnerability is 'Improper Authentication' (NVD, 2022) Kerberos can be used with Samba, which allows for Linux and Windows systems to share files between each other, it can also be used in the authentication of active directory domain users to a domain controller.

The vulnerability affects the name-based authentication that Kerberos and Samba uses to authenticate domain users. If the domain controller did not "strictly require a Kerberos PAC" – which is how the domain controller identifies the current user's privileges – it could lead to the domain being fully compromised (Docs.microsoft.com. 2022.). This could be a potential avenue that the attackers may choose to exploit, due to the possibility of taking over the full domain.

3.2 CVE-2022-21920

The second vulnerability affects the windows of Kerberos specifically, with Windows 7/8/10 and 11 being affected as well as Windows Server 2008-2022. Overall, there are 39 affected windows products. It has a high severity score of 8.8 and is classified as an 'Improper Privilege Management' weakness (NVD, 2022). The vulnerability is the ability to escalate privileges from a non-privileged domain user to a domain admin.

The vulnerability has a **high** score due to the low attack complexity, low user privilege and lack of user interaction. It also has a high impact since the attacker will have full access to the network and sensitive data. The attacker would also be able to damage or maliciously modify the network and its contents. It has not yet been exploited and all products identified to contain the vulnerability have been patched (Msrc.microsoft.com. 2022).

3.3 CVE-2020-3125

The third vulnerability affects the Cisco Adaptive Security Appliance Software which uses Kerberos' authentication within VPN's, firewalls, and other networking aspects on a Cisco networking device such as routers. The attack has a **high** severity score of 8.1 and is classified as 'Improper Authentication' (NVD, 2022). The vulnerability allows an attacker to spoof the Kerberos domain controller and divert traffic towards it rather than the legitimate domain controller, thus gaining access to the network.

The vulnerability itself is performed by spoofing the server response to the corresponding cisco device – all the attacker needs is an authorised username for the service they are targeting and a spoofed Kerberos domain controller. The attacker will then attempt to log into the service whilst directing the network traffic to the spoofed domain controller. This will allow the attacker to log into the service with an incorrect/invalid password and gain access to the network. (Cisco, 2022)

4. Potential Attack Vectors

These attack vectors rely on Kerberos being improperly configured and are consistently used in red-team exercises. The most common attack vectors are kerberoasting, golden tickets, and brute-forcing user enumeration. Attackers would need to already have access to the network either

through a domain user account or a privileged account for the golden ticket attack. These attacks allow the attacker to escalate their privileges and access further areas within the network.

4.1 Kerberoasting

Kerberoasting targets accounts within the active directory that contain a service principal name (SPN) set, accounts which have SPN's are typically service accounts. The SPN is required, as when the attacker requests a ticket from the active directory for a user with an SPN – it will return the ticket with an NTLM hash of the user's password. The attacker can then attempt to crack the password offline and return to the network when they have the plaintext password.

Service accounts are less likely to have strong passwords or be changed regularly, this increases the likelihood of the attacker being able to crack the password. If the attacker successfully cracks the password, they can then access the resources that the service has access to. For example, if the webserver was compromised – the database can be accessed, and data stored within can be extracted.

4.2 Golden Tickets

The golden ticket account targets the KRBTGT account, which encrypts and signs all the Kerberos authentication tokens within the domain controller. The KRBTGT account password can only be changed by a privileged user such as a system administrator and the account name can never be changed. This makes the attack easier for the attacker to perform, it is also difficult to detect as any tokens signed by the KRBTGT appear as legitimate signatures and tokens.

For this attack to work, the attacker needs to have access to a privileged account that has access to the domain controller such as a system administrator. The attacker then logs into the domain controller and dumps the password hash for the KRBTGT account. They will then crack the password and have access to the 'golden ticket' which is the KRBTGT account. From here they can access any area of the network, including areas only users with the highest possible privileges can access.

5. Mitigation Recommendations

The following mitigations should be applied to protect the company from the vulnerabilities and attack techniques that have been discussed in this report. Due to the high severity of the vulnerabilities, as well as the possible devastation the vulnerabilities and attacks pose it is imperative that they should be applied immediately, and continually applied.

5.1 Software Updates

The CVE's that have been discussed were resolved by the vendor through a software update. When vulnerabilities are identified, vendors will fix the security issue through a software patch. This is then pushed in a software update, to fix the issue within company and individual's software. The vendor will explain within the update or patch notes which CVE is being resolved or temporarily patched and which product/service is affected.

Using the most up-to-date version of software prevents attacker's from manipulating known vulnerabilities. Attackers can also use dedicated tools like mimikatz and metasploit, which can find the software version of the application or service that they are trying to target, which can be used to find vulnerabilities that have not been patched or resolved. It is imperative that whenever a software update is available it is downloaded and applied. If the software update is not applied, the application or service will still be vulnerable to the discovered vulnerabilities.

5.2 Password Policies

Password policies are likely already in place within the company and may differ depending on the type of account and authentication required. This section will be discussing password policies in terms of kerberos and employees of ScottishGlen. A recommended password policy would be enforcing the following:

Policy Recommendation	Suitable for Kerberos Authentication Protocol	Suitable for employees
Minimum Password Length	Yes	Yes
Maximum Password Age	**Yes – for certain accounts**	**No**
Password Complexity (Uppercase, Lowercase, Numeric and Nonalphanumeric)	Yes	Yes
Number of Invalid Password Attempts	Yes	Yes
Lockout and duration of lockout	Yes	Yes

Table 1 - Table containing recommended password policies

A minimum password length ensures that the password entropy is high enough that the difficulty to guess or crack the password is too difficult and deter the attacker. It has been recommended that a minimum password length is enforced rather than enforcing password complexity, as it leads to insecure passwords with low entropy being created such as 'P@55w0rd!'. A complexity requirement can be included, but passphrases such as 'MarbleButterflyJungle!01' should be recommended to ensure that the overall entropy of the password being used is high, whilst also enabling a more memorable password that the user can remember. Kerberos and Active Directory accounts that are privileged such as the KRBTGT account should enforce even higher minimum password lengths – again to increase the entropy of the password and make it more difficult to crack the password.

In terms of maximum password age, the recommendation may not be suitable for employee accounts and user accounts within Kerberos/Active Directory due to password hygiene issues. If users are being forced to change their password continuously, they will resort to using the same password with a different character, or weaker passwords that are easier to remember. It is recommended that user accounts only change their passwords if they are potentially or have been compromised. A maximum password age should be used with Kerberos and Active Directory privileged accounts, such as KRBTGT and service accounts. This prevents attackers from using previously cracked passwords to access the network.

To prevent attackers from attempting to brute-force their way into the network, a lockout policy should be in place. This would allow a user to enter their password in for a set number of times, for example three – before locking them out. The policy should then either freeze the account for a set amount of time or freeze the account with the administrator having to review the account and unlock it. Normal user accounts should be locked out for a set amount of time, whilst privileged accounts such as admins, KRBTGT accounts and other potentially sensitive accounts may benefit from being locked out until an admin can review the account.

5.3 Monitor Active Directory and Network Activity

The Active Directory and Network traffic can be monitored and analysed for any malicious or abnormal activity. Network logs should be monitored using security information and event management (SIEM) tools such as Splunk, LogRhythm or Sentinel. These tools allow for real-time

monitoring meaning possible intrusions are detected as they happen and can be managed before the attacker is able to escalate their privileges and move through the network.

A limitation of these tools is that they do require a level of learning by the analyst responsible for the SIEM. This learning will require time and money to implement, however it is worthwhile for the company to implement as it will save time and money in the future. These tools should be implemented immediately to ensure that potential attacks are identified and mitigated before they cause damage to the company and systems. For the vulnerabilities and attacks discussed, the use of a KRBTGT honeypot may be worthwhile – this will likely attract the attacker's attention rather than an actual KRBTGT account whilst highlighting that they are attempting to access or escalate through the network.

5.4 Restriction of KRBTGT Access

To prevent against golden ticket attacks, it is recommended that the only accounts that should be able access the password hash for the KRBTGT account, are those that absolutely need to have access. The only accounts that should have access is the domain admin and accounts that provide logon rights. If accounts that do not have these rights or accesses are able to access the KRBTGT or the domain admin and logon rights, this could be evidence that an attacker has been able to access the network and should be isolated.

References

Cve.mitre.org. 2022. CVE - CVE. [online] Available at: <https://cve.mitre.org/index.html> [Accessed 11 March 2022].

Cve.mitre.org. 2022. CVE -CVE-2020-25719. [online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25719> [Accessed 11 March 2022].

Cve.mitre.org. 2022. CVE -CVE-2020-3125. [online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3125> [Accessed 17 March 2022].

Cve.mitre.org. 2022. CVE -CVE-2022-21920. [online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21920> [Accessed 11 March 2022].

Docs.microsoft.com. 2022. [MS-APDS]: Kerberos PAC Validation. [online] Available at: <https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-apds/1d1f2b0c-8e8a-4d2a-8665-508d04976f84> [Accessed 11 March 2022].

Editor, N., 2022. Summary of the NIST Password Recommendations for 2021 - NetSec.News. [online] NetSec.News. Available at: <https://www.netsec.news/summary-of-the-nist-password-recommendations-for-2021/> [Accessed 21 March 2022].

FireEye. 2022. What is SIEM and how does it work? | FireEye. [online] Available at: <https://www.fireeye.com/products/helix/what-is-siem-and-how-does-it-work.html> [Accessed 21 March 2022].

Msrc.microsoft.com. 2022. Security Update Guide - Microsoft Security Response Center. [online] Available at: <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21920> [Accessed 11 March 2022].

Nvd.nist.gov. 2022. NVD - CVE- CVE-2020-25719. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2020-25719> [Accessed 11 March 2022].

Nvd.nist.gov. 2022. NVD - CVE-2020-3125. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2020-3125#match-4993826> [Accessed 17 March 2022].

Nvd.nist.gov. 2022. NVD - CVE-2022-21920. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2022-21920> [Accessed 11 March 2022].

Room362.com. 2022. Kerberoasting - Part 1 :: malicious.link — welcome. [online] Available at: <https://room362.com/post/2016/kerberoast-pt1/> [Accessed 20 March 2022].

simplilearn. 2022. What Is Kerberos, How Does It Work, and What Is It Used For?. [online] Available at: <https://www.simplilearn.com/what-is-kerberos-article> [Accessed 10 March 2022].

Tools.cisco.com. 2022. Cisco Adaptive Security Appliance Software Kerberos Authentication Bypass Vulnerability. [online] Available at: <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-asa-kerberos-bypass-96Gghe2sS> [Accessed 17 March 2022].

Varonis.com. 2022. Kerberos Attack: How to Stop Golden Tickets?. [online] Available at: <https://www.varonis.com/blog/kerberos-how-to-stop-golden-tickets> [Accessed 20 March 2022].

Wiki.samba.org. 2022. Running a Samba AD DC with MIT Kerberos KDC - SambaWiki. [online] Available at: <https://wiki.samba.org/index.php/Running_a_Samba_AD_DC_with_MIT_Kerberos_KDC> [Accessed 11 March 2022].